WHAT IS CLAIMED IS:

1	1. A method for detecting hostile software in a computer system		
2	comprising:		
3	storing a representation of configuration data associated with an		
4	operating system for the computer system obtained at a first time;		
5	comparing the stored representation of the configuration data obtained at		
6	the first time with a representation of the configuration data associated with the		
7	operating system for the computer system obtained at a second time; and		
8	if deviation is detected between the stored representation of the		
9	configuration data obtained at the first time and the representation of the configuration		
10	data obtained at the second time, automatically performing at least one remedial		
11	measure in response to the deviation detected.		
1	2. The method of claim 1 wherein the configuration data relates to		
2	identification of executable code installed in the computer system.		
_	radiametrical of executable code instance in the comparer system.		
1	3. The method of claim 1 wherein the configuration data relates to		
2	identification of a command line for invoking executable code associated with a		
3	particular file extension.		
1	4. The method of claim 1 wherein the configuration data is obtained		
2	from a registry maintained by the operating system.		
-	Louis a region, managed by the op themself by the second		
1	5. The method of claim 4 wherein the configuration data obtained		
2	from at least one key associated with the registry.		
1	6. The method of claim 1 wherein the configuration data is obtained		
2	from a file stored in the computer system.		
_	nom a me dicrea m me comparer of com.		
1	7. The method of claim 1 wherein the stored representation of		
2	configuration data is encoded prior to being stored.		
1	8. The method of claim 1 wherein the configuration data is		
2	compared to a predefined value.		
_	compared to a production ratio.		

1	9	•	The method of claim I wherein the configuration data is checked		
2	for addition of d	lata.			
1	1	0.	The method of claim 1 wherein the configuration data is checked		
2	for removal of d				
	_	_			
1		1.	The method of claim 1 wherein the at least one remedial measure		
2	comprises determining a storage location associated with suspected executable code in				
3	the computer sy	stem.			
1	1	2.	The method of claim 1 wherein the at least one remedial measure		
2	comprises deter	minin	g whether suspected executable code is currently executing.		
1	1	3.	The method of claim 12 wherein the at least one remedial		
2	measure further	comp	rises terminating execution of the suspected executable code.		
1		4.	The method of claim 13, wherein the suspected executable code		
2	does not receive	notif	ication prior to being terminated.		
1	1	5.	The method of claim 1 wherein the at least one remedial measure		
2	comprises moving suspected executable code to a specified storage location for later				
3	evaluation.				
1	1	6.	The method of claim 1 wherein the at least one remedial measure		
2	comprises altering configuration data associated with the operating system to reflect the				
3	stored representation of the configuration data.				
1	1	7	The method of claim 1 subgrain the energting system is a		
1		7.	The method of claim 1 wherein the operating system is a		
2	Windows-based	. opera	ating system.		
1	1	8.	The method of claim 1 wherein the operating system is a Linux-		
2	based operating	syste	m.		
1	1	9.	A computer system capable of detecting hostile software		
2	comprising:	- •	,		
3		nroce	essing unit canable of being controlled by an operating system:		

4	a storage unit coupled to the processing unit, the storage unit capable of		
5	storing a representation of configuration data associated with the operating system		
6	obtained at a first time;		
7	wherein the processing unit is capable of comparing the stored		
8	representation of the configuration data obtained at the first time with a representation		
9	of the configuration data associated with the operating system obtained at a second time		
10	and, if deviation is detected between the stored representation of the configuration data		
11	obtained at the first time and the representation of the configuration data obtained at the		
12	second time, automatically performing at least one remedial measure in response to the		
13	deviation detected.		
1	20. A system for detecting hostile software in a computer system		
2	comprising:		
3	means for storing a representation of configuration data associated with		
4	an operating system for the computer system obtained at a first time;		
5	means for comparing the stored representation of the configuration data		
6	obtained at the first time with a representation of the configuration data associated with		
7	the operating system for the computer system obtained at a second time; and		
8	means for automatically performing at least one remedial measure in		
9	response to the deviation detected, if deviation is detected between the stored		
10	representation of the configuration data obtained at the first time and the representation		
11	of the configuration data obtained at the second time.		
1	21. An article of manufacture comprising:		
2	a computer usable medium having computer readable program code		
3	means embodied therein for causing hostile software to be detected in a computer		
4	system, the computer readable program code means in said article of manufacture		
5	comprising:		
6	computer readable program code means for causing a computer to store		
7	a representation of configuration data associated with an operating system for the		
8	computer system obtained at a first time;		
9	computer readable program code means for causing the computer to		
10	compare the stored representation of the configuration data obtained at the first time		

with a representation of the configuration data associated with the operating system for
the computer system obtained at a second time; and
computer readable program code means for causing the computer to
automatically perform at least one remedial measure in response to the deviation
detected, if deviation is detected between the stored representation of the configuration
data obtained at the first time and the representation of the configuration data obtained
at the second time.